Alice

Bob

Information Security and Privacy Advisory Board

IDENTITY MANAGEMENT FRAMEWORK

02 April 2009

INTRODUCTION

- The topic of Identity Management was discussed at the December 2008 ISPAB Mtg.
- Elaine Newton of NIST described several activities underway touching upon ID Mgmt.
- Request was made to provide guidance for identity management efforts

IDENTITY MANAGEMENT – *ONE DEFINITION*

- The set of operations associated with the life-cycle maintenance of attributes associated with an entity
  - Operations, policies and technologies
  - Inclusive of non-human entities
  - Covering *creation* through *destruction (beyond?)*

NIST: An Identity Management System is any system that creates, issues, uses, and terminates *electronic* identities. In other words, an Identity Management System provides lifecycle management for the digital credential sets that represent electronic identities.

"On the Internet, nobody knows you're a dog."

NIST AND IDENTITY MANAGEMENT

- NIST has already produced bodies of work on identity issues such as:
  - SP 800-103 : An Ontology of Identity Credentials, Part I: Background and Formulation (DRAFT)
  - SP 800-63 : Electronic Authentication Guidelines
  - Several SPs related to PIV
- Other activities
  - Global eID
- So where's the gap?

ASSESSING THE GAP

- Need to assess the state of both traditional and evolving identity frameworks
  - Within government
  - In industry and academia
- The past decade has been filled with many efforts
  - CardSpace (Microsoft)
  - OASIS (SAML 1 & 2, XACML)
  - Liberty Alliance
  - WS*
  - OpenID, OAuth, and others
- What is the applicability of such efforts for government use?

LIBERTY ALLIANCE (JUST AN EXAMPLE)

- ID Federation Framework (leading to SAML 2)
  - Related work: OpenID, SAML
  - Using Identity across disparate boundaries
- ID Web Services Framework
  - Building Identity Centric Core Services, XACML
- ID Governance Framework
  - Related work: OAuth, Merkle Hash Trees
  - Portable identity attribute use policies
- ID Assurance Framework (building upon 800-63)
  - Normalization of Identity *value*
- ID Service Interface Specification
  - Foundation abstraction to allow unique ID driven services

WHAT SHOULD NIST DO?

- Some proposed discussion topics include;
  - Create a means to evaluate identity management frameworks
    - Their similarities and differences
    - In abstract terms that can cover the ID “universe”
  - Identification of the interoperability of various identity schemes
  - Catalog relevant identity related technologies and where they fit in the assessment framework